IN THE CLAIMS:

Please cancel claims 1-23 without prejudice or disclaimer, and substitute new Claims 21-46 therefor as follows:

Claims 1-23 (Cancelled).

24. (New) A user authentication method based on the use of identification biometric techniques comprising an enrolment step and a verification step, said enrolment step comprising the steps of:

generating a reference biometric template from a first biometric image of a user to be authenticated;

splitting said reference biometric template into a first and a second reference biometric template portion;

enciphering said first and second reference biometric template portion; and

storing each one of said reference biometric template portions into a different memory.

25. (New) The method according to claim 24, wherein said step of storing each one of said reference biometric template portions into a different memory comprises the step of:

transmitting said first reference biometric template portion from a first system to a device, said first system operating in said enrolment step;

storing said first reference biometric template portion into a memory of said device, said device operating in said verification step;

transmitting said second reference biometric template portion from said first system to a second system, said second system operating in said verification step; and

storing said second reference biometric template portion into a memory of said second system.

26. (New) The method according to claim 24, wherein said verification step comprises the steps of:

generating a live template from a second biometric image of said user to be authenticated;

enciphering said live template; and

transmitting said live template and said second reference biometric template portion to said device.

27. (New) The method according to claim 26, wherein said verification step comprises the steps of:

deciphering said live template and said second reference biometric template portion;

recomposing said reference biometric template from said first and second reference biometric template portion; and

comparing said recomposed reference biometric template with said live template.

28. (New) The method according to claim 27, wherein said verification step comprises the steps of:

sending a result of said comparison to said second system; and

authenticating or not authenticating said user depending on said result.

29. (New) The method according to claim 25, wherein said step of splitting said reference biometric template into a first and a second reference biometric template portion comprises the step of:

destroying said biometric template performed by said first system.

30. (New) The method according to claim 25, wherein said step of enciphering said first and second reference biometric template portion comprises the steps of:

storing a first and a second key and a related digital certificate into a memory of said first system, said first and second keys being respectively a public key and a private key associated with said first system;

storing a first and a second key and a related digital certificate into said memory of said device, said first and second keys being respectively a public key and a private key associated with said user to be authenticated;

signing said first and second reference biometric template portion with said private key of said first system; and

enciphering said, first and second reference biometric template portion with said public key of said user to be authenticated.

31. (New) The method according to claim 26, wherein said step of transmitting said live template and said second reference biometric template portion to said device comprises the steps of:

generating an aleatory value associated with the current data verification step, said aleatory value guaranteeing the authenticity of said current data verification step;

signing and enciphering said aleatory value; and

transmitting said aleatory value to said device.

32. (New) The method according to claim 30, wherein said step of enciphering said comparison biometric template comprises the steps of:

storing a first and a second key and a related digital certificate into said memory of said second system, said first and second keys being respectively a public key and a private key associated with said second system;

signing said live template with said private key of said second system; and

enciphering said live template with said public key of said user to be authenticated.

33. (New) The method according to claim 31, wherein said step of deciphering said live template and said second reference biometric template portion comprises the steps of:

deciphering the signature and the validity of said aleatory value;

deciphering said second reference biometric template portion with said private key of said user to be authenticated;

verifying its signature;

deciphering said live template with said private key of said user to be authenticated; and

verifying its signature.

34. (New) The method according to claim 28, wherein said step of sending a result of said comparison to said second device comprises the steps of:

generating a message containing said result; and

enciphering said message.

35. (New) The method according to claim 24, wherein said identification biometric techniques comprise at least one biometric identification technique of the type selected from:

face recognition, fingerprints, hand prints, voice templates, retinal images, and calligraphic samples.

36. (New) The method according to claim 25, wherein said first and second systems are respectively a data enrolment system and a data verification system and said device is a data carrier.

37. (New) The method according to claim 24, wherein said step of splitting said reference biometric template comprises the step of:

splitting said reference biometric template into a plurality of reference biometric template portions, at least some of said reference biometric template portions being used to recompose said reference biometric template.

38. (New) A user authentication architecture based on the use of biometric identification techniques comprising:

at least one data enrolment system for generating a reference biometric template from a first biometric image of a user to be authenticated, said data enrolment system comprising a host computer to split said reference biometric template into a first and a second reference biometric template portion and for enciphering said first and second reference biometric template portion;

at least one portable data carrier associated with said user to be authenticated, said data carrier comprising a memory for storing said first signed and enciphered reference biometric template portion; and

at least one data verification system comprising a memory for storing said second signed and enciphered reference biometric template portion.

39. (New) The user authentication architecture according to claim 38, wherein said data carrier comprises a microprocessor comprising a processing logic for deciphering said first and second reference biometric template portion, verifying the signature and recomposing said reference biometric template from said first and second deciphered reference biometric template portion.

40. (New) The user authentication architecture according to claim 39, wherein said microprocessor comprises a comparing logic to compare said recomposed reference biometric template with a live template generated by a second biometric image of the user to be authenticated, said second biometric image of the user to be authenticated being generated by the data verification system.

41. (New) A portable data carrier associated with a user that has to be authenticated through a user authentication architecture, said data carrier comprising a microprocessor comprising a memory for storing a first reference biometric template portion associated with said user to be authenticated, said first reference biometric template portion being signed and enciphered, said portable data carrier being adapted to receive as input, from said user authentication architecture, a second reference biometric template portion and a live template associated with said user to be authenticated, said second reference biometric template portion and said live template being signed and enciphered, said microprocessor further comprising:

a processing logic for deciphering said first and second reference biometric template portions and for recomposing therefrom said reference biometric template associated with said user to be authenticated; and

a comparing logic for comparing said reference biometric template recomposed with said live template and sending a result of said comparison to said user authentication architecture.

42. (New) The portable data carrier according to claim 41, comprising a substrate whose sizes are substantially rectangular.

43. (New) The portable data carrier according to claim 41, wherein said data carrier is an access card or a credit card or a debit card or an identification card or a smart card or a SIM card.

44. (New) A data verification system comprising an electronic device and a portable data carrier associated with a user that has to be authenticated, said data carrier being adapted to store a first reference biometric template portion associated with a user to be authenticated, said first reference biometric template portion being signed and enciphered;

said electronic device comprising:

a memory adapted to store a second reference biometric template portion associated with a user to be authenticated, complementary to said first portion, said second reference biometric template portion being signed and enciphered;

an image acquiring and processing device for generating a live template;

said electronic device being adapted to encipher and sign said live template, transmitting said second reference biometric template portion and said live template to

said portable data carrier and authenticating said user depending on the result of a comparison performed by said data carrier between said live template and a reference biometric template of said user to be authenticated, said reference biometric template being rebuilt by using said first and second reference biometric template portion.

45. (New) A data verification system comprising an electronic device and, a portable data carrier associated with a user that has to be authenticated, said data carrier being adapted to store a first reference biometric template portion associated with a user to be authenticated, said first reference biometric template portion being signed and enciphered;

said electronic device comprising:

a first memory adapted to store a second reference biometric template portion associated with a user to be authenticated, said second reference biometric template portion being signed and enciphered;

at least a second memory adapted to store at least a third reference biometric template portion associated with a user to be authenticated, said third reference biometric template portion being signed and enciphered, wherein said first, second and at least third reference biometric template portions are such that the reference biometric template can be recomposed from a subset of at least two of said reference biometric template portions;

an image acquiring and processing device for generating a live template;

said electronic device being adapted to encipher and sign said live template, transmitting said second reference biometric template portion and said live template to said portable data carrier and authenticating said user depending on the result of a

comparison performed by said data carrier between said live template and a reference biometric template of said user to be authenticated, said reference biometric template being rebuilt by using said first and second reference biometric template portion.

46. (New) A program for an electronic processor that can be loaded into the memory of at least one electronic processor and comprising program codes for performing the steps of the method according to claim 24, when said program is capable of being executed by said electronic processor.